CLAIMS:

1. A method of protecting content stored on a storage medium against unauthorised access, said storage medium being accessible by a drive (D) of a portable device which is connectable to a network (1), comprising the steps of:
- transmitting an identifier (id) of said storage medium or the user to an authentication unit (Auc) within said portable device or within said network,
- generating a cryptographic key (ck) using said identifier (id) and an authentication key (ak) by an authentication algorithm within said authentication unit (Auc),
- transmitting said cryptographic key (ck) from said authentication unit (Auc) to said drive (D),
- encrypting the content to be protected using said cryptographic key (ck), and
- storing the encrypted content on said storage medium.

2. A method as claimed in claim 1, wherein said identifier (id) is stored on said storage medium in machine-readable form and is read before transmission to said authentication unit (Auc).

3. A method as claimed in claim 1, wherein said authentication unit is part of said portable device.

4. A method as claimed in claim 1, wherein said authentication key (ak) is stored within said authentication unit or on a removable authentication memory, in particular a SIM card, which is readable by said authentication unit.

5. A method as claimed in claim 1, wherein said authentication unit (Auc) is part of said network.

6. A method as claimed in claim 1, wherein said storage medium is a removable record carrier, such as an optical disk, a removable hard disk or a semiconductor memory

card.

7. A method as claimed in claim 1, wherein said storage medium is a non-removable storage medium, such as a semiconductor memory or a non-removable hard disk.

8. A method as claimed in claim 1, wherein said portable device is a mobile phone, wherein said authentication unit is a SIM card reader, wherein said network is a mobile phone network and wherein said authentication algorithm corresponds to the algorithm used by said mobile phone network for authenticating mobile phones.

9. A method as claimed in claim 8, wherein said identifier (id) is the PIN of the user.

10. A method as claimed in claim 1, wherein said identifier (id) is transmitted from said portable device to said authentication unit (Auc) via the internet and a link from the internet to said network, in particular via a computer connected to the internet.

11. A device for protecting content stored on a storage medium against unauthorized access, said storage medium storing a machine-readable identifier (id), said device comprising:

- means for connecting said device to a network,
- a drive (D) for accessing said storage medium, in particular for reading content from and writing content to said storage medium,
- a transmitter for transmitting an identifier (id) of said storage medium or the user to an authentication unit (Auc) within said device or within said network,
- a receiver for receiving a cryptographic key (ck) generated within said authentication unit (Auc) by an authentication algorithm using said identifier (id) and an authentication key (ak) and for transmitting said cryptographic key (ck) to said drive (D), and
- encryption means (D) for encrypting content to be protected using said cryptographic key (ck) for storage on said storage medium.

12. A method of accessing content stored in encrypted form on a storage medium, said storage medium being accessible by a drive (D) of a portable device which is connectable to a network, comprising the steps of:

- transmitting an identifier (id) of said storage medium or the user to an authentication unit (Auc) within said portable device or within said network,
- generating a cryptographic key (ck) using said identifier (id) and an authentication key (ak) by an authentication algorithm within said authentication unit (Auc),
- transmitting said cryptographic key (ck) from said authentication unit (Auc) to said drive (D), and
- decrypting the content to be accessed using said cryptographic key (ck).

13. A device for accessing content stored on a storage medium against unauthorized access comprising:
- means for connecting said device to a network,
- a drive (D) for accessing said storage medium, in particular for reading content from and writing content to said storage medium,
- a transmitter for transmitting an identifier (id) of said storage medium or the user to an authentication unit (Auc) within said device or within said network,
- a receiver for receiving a cryptographic key (ck) generated within said authentication unit (Auc) by an authentication algorithm using said identifier (id) and an authentication key (ck) and for transmitting said cryptographic key (ck) to said drive (D), and
- decryption means (D) for decrypting content to be accessed using said cryptographic key (ck).

14. Device as claimed in claim 11 or 13, wherein said device is a mobile phone, wherein said authentication unit is a SIM card reader, wherein said network is a mobile phone network and wherein said authentication algorithm corresponds to the algorithm used by said mobile phone network for authenticating mobile phones.

15. Computer program comprising computer program code means for causing a computer to perform the steps of the method as claimed in claim 1 or 12 when said program is run on a computer.